Chief Health Informatics Office
Emerging Health Technologies

Role-Based Access Control (RBAC) Newsletter

Volume 37 – January 2008

Inside this Issue:

Robert O'Hara, MD
VHA/IHS RBAC TF Chair
Robert.OHara@va.gov

Steve Wagner
VHA Deputy Chief Architect
RBAC Project Manager
Steve.Wagner@va.gov

Mike Davis, CISSP
VHA Security Architect
RBAC Architect
Mike.Davis@va.gov

Ed Coyne, PhD
VHA Security Architect
RBAC Architect
Ed.Coyne@va.gov

Suzanne Webb
RBAC Project Lead
Information Security Analyst
Suzanne.Gonzales-Webb@va.gov

Notification on Final Action of: ANSI/HL7 V3 RBAC, R1-2008

HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, Release 1 **(new standard)**

Approval Date of Final Action: 2/20/2008

The Board of Standards Review has approved the above action in connection with a candidate American National Standard:

Notice of this Final Action will be published in an upcoming issue of Standards Action. For actions other than withdrawals, applicable publication and maintenance requirements are contained in clause four of the ANSI Essential Requirements: Due process requirements for American National Standards.

Note from Mike Davis: *Congrats on this achievement in the creation of a worldwide RBAC standard!! You all should be justifiably proud of your contribution to healthcare security. I am particularly grateful for the dedicated efforts of the clinical community that worked so diligently and so long in the RBAC TF to make this possible.*

HEALTH LEVEL SEVEN (HL7) WORKING GROUP MEETING

January 2008 – San Antonio, Texas

Role Based Access Control – HL7 Ballot Passes

More Congratulations as the Security Technical Committee also proudly announces the passing of the Role-Based Access Control (RBAC) Permission Catalog as an HL7 standard. During the ballot process it was determined that additional vocabulary would be added. The decision to add this vocabulary was agreed upon by HL7 voting members. In support of this new work item, European and ISO information from Bernd Blobel, co-chair of the Security TC, will also be provided. Glen Marshall, co-chair of the Security TC, will be participating in discussions with the HL7 vocabulary co-chairs to determine the process to go forward in proceeding with publication and continued maintenance of the vocabulary.

Upcoming Meetings

- **INCITS CS1 Mtg #13**
  (ITI-INCITS HQ)
  February 27-28, 2008
  Washington, DC
- **INFOSEC World Conference**
  March 10-12, 2008
  Orlando, FL
- **The 5th Annual World Health Care Congress**
  April 21–23, 2008
  Washington, DC
- **HL7 Working Group**
  May 4-9, 2008
  Phoenix, AZ
- **TEPR 2008**
  May 17–21, 2008
  Ft. Lauderdale, FL
- **17th Annual WEDI National Conference**
  May 19–22, 2008
  Baltimore, MD

RBAC Newsletter

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

HL7 Project Initiation for Constraints, Constraint Project Status

A motion was passed in September 2007 by the Security Technical Committee to initiate a project for constraints, including the coordination with the ISO PMAC policy standard. This project will also focus on closing the HITSP and other identified gaps for standards to communicate privacy policies. At the San Antonio HL7 Working Group meeting the Security TC decided to combine constraints project work with joint project work for Privacy and Consents with the Community Based Collaborative Care or CBCC special interest group. This task has been assigned to Mike Davis and Suzanne Gonzales-Webb to proceed. The joint work will include coordination with the ISO PMAC[1] policy standard to include constraints. The Security TC will also be focusing on closing the identified HITSP[2] and other standard organizational gaps in communication of privacy policies.

Using the definition from Neumann and Strembeck, constraints are restrictions (conditions or obligations) that are enforced upon access permissions. In RBAC, a constraint may restrict for example, a user to continue to have an *action* on the data they are accessing. This could include contextual properties such as separation of duties, time-dependency, mutual exclusivity, cardinality, location, etc.

For complex healthcare environments, constraints provide the higher flexibility required in RBAC implementation.

One has to ask first, in dealing with constraints with respect to access control, which parts of these unmanageable quantities of context information are relevant for a specific authorization decision, and how the corresponding information may be elicited and defined on the modeling level. In the Constraint document posted on the RBAC website, we suggest a process for the specification of context constraints. This process is based as an extension to the scenario-driven role engineering process for RBAC roles presented in Neumann and Strembeck.[3]

In Role-Based Access Control, users (i.e., individuals or authorization services, etc.) are given a set of permissions (the ability to have an action such as create, read, write, etc.) on an object (a laboratory order, patient history, etc.). In a healthcare environment arena however,

[1] ISO PMAC - International Organization for Standardization Privilege Management and Access Control
[2] HITSP – Health Information Technology Standards Panel
[3] M. Strembeck and G. Neumann, An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments; Received November 2003; revised March 2004, April 2004 and May 2004; accepted May 2004

Upcoming Meetings

- **IEEE Security & Privacy Symposium**
  May 21-24, 2008
  Berkeley/Oakland, CA
- **13th ACM SACMAT**
  June 11-13, 2008
  Estes Park, CO

increased flexibility in RBAC is needed as the duties and functions of identified structural roles such as a physician, nurse or pharmacist[4] in relation to accessing an information system can vary on the time of day, their location (i.e., clinic, ward) and when the additional temporary duties are assigned (i.e., supervisory or administrative). These conditional changes or constraints modify the level of access control an individual user may have. One possibility to deal with this dynamically changing context is to rapidly modify permission assignment relations according to the changes in the (healthcare) environment. This central idea supports constraints on almost all parts of an RBAC model (e.g., permissions, roles, or assignment relations) to achieve a high flexibility.[5]

Conditional Privacy-Aware Role Based Access Control[6]

Qun Ni, Dan Lin, Elisa Bertino[7] and Jorge Lobo[8]

In this abstract, the group of authors introduces a family of models they name as P-RBAC (Conditional Privacy-aware Role Based Access Control) that extends the current familiar RBAC model in order to fully support and express privacy policies, while also taking account features such as purposes and obligations.

Introduction

Privacy today is a key issue in information technology (IT)[9] and has received increasing attention from consumers, stakeholders, and legislators. Legislative acts, such as the Health Insurance Portability and Accountability Act (HIPAA)[10] for healthcare require enterprises to protect the privacy of their customers. In attempts to address privacy, enterprises have adopted various strategies to protect customer data and to communicate their privacy policies to customers, such as publishing a privacy policy or policies on their website.[11] Those approaches however cannot truly safeguard consumers because they do not address

[4] Structural roles are categories of healthcare personnel warranting differing levels of access control. Structural roles allow a user to 'connect' to a resource, but do not grant authorization. Structural roles define what specific healthcare workflow users are allowed to participate in, while functional roles define authorizations granted to an entity to allow access (i.e., to protected health information).

[5] Ibid, M. Strembeck and G. Neumann

[6] Work reported in this paper has been partially supported by IBM under the OCR project "Privacy and Security Policy Management". Participants to this project are: Carnegie Mellon University, IBM T.J. Watson Research Center, and Purdue University.

[7] Dept of computer Science, Purdue University, w. Lafayette, IN 47907, USA

[8] IBM Watson Research Center, Hawthorne, NY 10598, USA

[9] S.W. Smith and E.H. Spafford. Grand challenges in information security: Process and output. *IEEE Security and Privacy*, pages 69-71, Jan 2004

[10] United States Department of Health. Available at http://www.hhs.gov/ocr/hipaa/.

[11] Amazon.com. Amazon privacy notice. http://www.amazon.com/exec/obidos/tg/browse/-/468496/102-8997954-0573735.

RBAC Newsletter

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

how consumer personal data is actually handled after it is collected. Enterprises' actual practice might intentionally or unintentionally violate the privacy policies published on their websites.

Per the authors, privacy protection can only be achieved by enforcing privacy policies within an enterprise's online and offline data processing systems and therefore consider enforceability of privacy policies as the key to a solution for privacy protection.

Abstract

Privacy is considered critical for all organizations needing to manage individual related information. As such, there is an increasing need for access control models which can adequately support the specification and enforcement of privacy policies. In this paper, the authors propose a model, referred to as Conditional Privacy-aware Role Based Access Control (P-RBAC), which supports expressive condition languages and flexible relations among permission assignments for more complex privacy policies. Efficient algorithms for detecting conflicts, redundancies, and indeterminism for a set of permission assignments are presented. In the paper the authors also extend Conditional P-RBAC to Universal P-RBAC by taking into account hierarchical relations among roles, data and purposes. In comparison with other approaches, such as Platform for Privacy Preference (P3P), Enterprise Privacy Authorization Language (EPAL), and eXtensible Access Control Markup Language (XACML), our work has achieved both expressiveness and efficiency.

Conclusion

The authors proposed Conditional P-RBAC and Universal P-RBAC for specifying complex privacy policies. The key design criterion is to balance efficiency and expressiveness. The definition of domains and atomic conditions are carefully chosen to reflect the wide needs for enforceable privacy policies and to meet our efficiency goal, so does the design of condition languages and permission assignment sets. The authors have taken into account the effect of hierarchical relations among roles, data and purposes, which further enhance the expressiveness of our approach. As part of future work, the authors plan to introduce a sticky policy paradigm[12] into P-RBAC and develop a formal method to describe and manage obligations and to automatically detect possible conflicts between obligations and between obligations and actions.

RBAC Newsletter

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov

[12] G. Karjoth, M. Schunter and M. Waiderner. Platform for enterprise privacy practices: Privacy-enabled management of customer data. In *Privacy Enhancing Technologies*, pages 69-84, 2002

RBAC Task Force – Meeting Update

In reviewing the negative resolutions of the HL7 Ballot, the RBAC Task Force has agreed that the addition of the role 'Patient' and 'Patient Advocate or designee') should be added to the RBAC Role Catalog. The resulting permissions associated with these roles will be worked on in the upcoming February meeting. The RBAC Task Force meeting calls are held on the **SECOND** Wednesday of every month at 1300CT / 1100PST / 1200MT / 1400EST and a meeting reminder is sent to current participants. If you would like to participate in the Task Force please contact Suzanne Gonzales-Webb for more information.

Role-Based Access Control is critically important to the security aspects of the Veterans Health Administration and to other organizations. There is a growing management and security demand for RBAC to be implemented.

RBAC grants rights and permissions to roles rather than individual users. Users then acquire the rights and permissions by being assigned to appropriate roles. By grouping individuals with other individuals who have similar access rights, RBAC can provide significant security management efficiencies.

The latest RBAC documentation additions and prior RBAC Newsletters can be found on the RBAC Website (http://www.va.gov/rbac/).

≈

The RBAC Newsletter is now published quarterly instead of monthly. Please be on the lookout for the next issue due March/April 2008!

RBAC Newsletter

ATTN: Suzanne Webb
RBAC Project Lead
10260 Campus Point MS-B1E
La Jolla, CA 92121

Or e-mail:

Suzanne.Gonzales-Webb@va.gov